

Testimony  
House Committee on Homeland Security  
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology  
“Cyber Security Recommendations for the Next Administration”  
James A. Lewis  
Center for Strategic and International Studies  
September 16, 2008

I thank the Committee for the opportunity to testify on the work of the CSIS Cybersecurity Commission on Cyber Security for the 44<sup>th</sup> Presidency. As you know, this Commission was established a year ago. It held its first meeting in November 2007. Our goal is to identify concrete actions that the next administration can take to improve cybersecurity. We are composed of forty individuals with extensive experience in cyber security and in government operations, and our work has been supported by a number of eminent experts in this field. We have also received invaluable assistance from the Department of Defense, the Intelligence Community, the FBI and from elements of the Department of Homeland Security. Let me also note that you, Mr. Chairman, and your colleague Representative McCaul, have provided essential support and guidance during the course of our work. Your leadership has been crucial for shaping the report and in moving the Commission forward.

The starting point for the Commission’s work was that the lack of cyber security and the loss of information were doing unacceptable damage to the United States. It has been ten years since the first reports called attention to America’s vulnerability in cyberspace. Unfortunately, the situation has gotten worse, not better, during the intervening decade. That cyberspace now provides the foundation for much of our economic activity is not readily apparent. However, those who wish to do harm to the U.S. have not failed to notice the opportunities created by the weaknesses of U.S. networks. There has been damaging losses of valuable information. These losses occurred in both the government and the private sector, creating major risks for national security and doing major damage to U.S. global competitiveness. We are also deeply concerned by the idea that these intruders, since they were able to successfully enter U.S. networks to steal information without being detected, could just as well be leaving something behind, malicious software that could be triggered in a crisis to disrupt critical services or infrastructure.

I should note that when we began our work, the Administration had not announced its National Cyber Security Initiative. We appreciate the willingness of some Departments to share the details of this highly classified activity to those of us who hold the appropriate clearances. As a group, we believe this initiative has begun to make a tremendous contribution to improving U.S. national security and we applaud those who are struggling to implement it. We have adjusted our work in light of the Initiative; it has brought progress, but there is still much work to be done.

The CSIS Cyber Commission hopes to have finished its work by November of this year. So our discussion today must necessarily reflect that in some instance, the group has not finished its work on key recommendations. What I and my colleagues can do, however, is brief the committee on the issues we have identified and some of the options we are considering.

Let me begin by noting our two most important findings. The first is that cyber security is now one of the most important national security challenges facing the U.S. This is not some

hypothetical catastrophe. We are under attack and taking damage. Our second finding is that the U.S. is not organized and lacks a coherent national strategy for addressing this challenge.

These two findings inform our work and our recommendations, and the Commission has identified several broad areas where we recommend that the next administration take immediate action. These are to develop a comprehensive national security strategy for cyber space; to reorganize the governance of cyberspace to provide accountability and authority; to rebuild relationships with the private sector; to modernize cyberspace authorities; and use regulation and federal acquisitions to shape markets.

## **National Strategy**

In light of our conclusion that cyberspace must now be part of that national security strategy, our recommendations call for the use of all instruments of U.S. power to secure cyberspace. We identify five principle instruments – diplomatic, military, economic, law enforcement and intelligence – to achieve this and will recommend that the next administration make use of them in a coordinated and well-resourced national approach.

## **Diplomatic Initiatives**

The diplomatic aspects of cyber security have been among the least developed elements of U.S. policy. Our vision of a diplomatic strategy involves advocacy, cooperation and norms. It is patterned after the U.S. experience in building international cooperation in non-proliferation. Increasingly, all nations and all peoples depend on cyberspace to conduct their daily affairs and this provides opportunities for cooperation. We will recommend that the U.S. advocate measure to secure cyberspace in every multilateral initiative where it is appropriate, just as we have advocated measure to advance nonproliferation or to combat terrorism.

## **Military and Defense**

Much of the discussion of the military aspects of cybersecurity is necessarily classified. This limits what our Commission can say on offensive information warfare. However, we discussed several essential topics. These included how to improve deterrence, how to link strategy to an appropriate doctrine for use, and how to train and equip forces. The most important conclusion we reached is that credible offensive capabilities is necessary to deter potential attackers.

The U.S. has a doctrine for military operations in cyberspace, but we believe this doctrine will need to be expanded if it is to be effective. Doctrine provides guidance on the exercise of the various and overlapping legal authorities that apply to cyberspace, identifying when the use of law enforcement, military or intelligence authorities are appropriate. An expanded doctrine should specify relationships among agencies and lay out the decision-making process for various actions. Our initial conclusion is that the next administration should refine existing doctrine and create processes to work through the issues of deterrence and strategic operations in cyberspace.

## **Economic tools**

Our review suggests that the U.S would benefit from making greater use of the economic tools available to it. These tools include using international economic programs and organizations to

promote cyber security, to develop norms and sanctions for international behavior, to work with international standards bodies and to invest in research and development in cybersecurity. A concrete example of this would be our bilateral trade negotiations with Russia. While the Russians had to improve their performance to many legal and trade requirements, they were not asked for better national performance in securing cyberspace. This must change.

## **Intelligence and Law Enforcement**

Our review of cyber security efforts found that the intelligence community has led the efforts to improve U.S. national cyber security. To foreshadow our discussion of organizational issues, we considered recommending that the intelligence community be formally given the lead role in securing cyber space, but ultimately decided that this would be politically infeasible. Our recommendations emphasize that its primary role in securing cyberspace will be to support diplomatic, military, and domestic elements of a comprehensive strategy.

We were also impressed by the work of the Federal law enforcement community. Our recommendations will emphasize that an important activity for law enforcement is to work with other nations, as part of a larger diplomatic strategy, to shrink the 'sanctuaries' available for cybercrime. Another essential law enforcement function is to ensure adequate protections for privacy and civil liberties in any cyber initiative. A comprehensive response to cyber attack need not come at the expense of civil liberties, and success will depend in some measure on the ability of the government to assure Americans that their rights are being safeguarded. We believe this assurance requires a commitment from the White House and vigorous Congressional oversight.

We believe that the new administration has an opportunity to build on the NCSI to create a coherent national strategy. This strategy should be one of the first policy documents that it issues. Moving to a strategy for cyber space that focuses on using all the tools of national power creates an important challenge however. We found that the current ability to organize and coordinate the use of diplomatic, military, economic, intelligence and law enforcement activities is inadequate. This will need to change improve cyber security.

## **Organization**

It did not take long for our group to conclude that our national efforts in cyberspace are disorganized. None of the existing cyber security structures are adequate. We found that the central problems in the current Federal organization for cyber security are the lack of a strategic focus, overlapping missions, poor coordination and collaboration, and diffuse responsibility. Much of the problem resides with the performance and capabilities of the Department of Homeland Security. While the Department's performance has improved in recent years, making this Department more effective will be an immediate task for the next administration. However, our view is that any improvement to the nation's cyber security must go outside of DHS to be effective, and this will require rethinking the roles of DHS and the Homeland Security Council.

Given DHS's weaknesses, we considered a number of alternatives. The Intelligence community has the necessary capabilities but giving it a lead role poses serious constitutional problems. DOD is well suited to manage a national mission, but giving it the lead suggests a militarization of cyber space. We concluded that only the White House has the necessary authority and oversight for cyber security.

Simply appointing a czar, however, will not work. Czars in Washington tend to be either temporary or marginalized. Longing for a Czar is a symptom of our industrial-age governmental organization. We are developing recommendations on how to leverage information technology to increase security while improving the efficiency, and transparency of government operations. Our thinking on this has been shaped in part by the implementation of the Intelligence Reform and Terrorist Prevention Act, which imposed a new, more collaborative structure on the Intelligence Community. This is still a work in progress, but the IC's experience shows that the combination of a Congressional mandate, adequate authorities, and a focus on "enterprise" solutions (e.g. those that cut across traditional agency barriers) can improve federal performance.

We believe that the next administration's response to the cyber security challenge provides an opportunity to test new approaches to federal organization that better leverage the use of cyberspace and social networking technologies to improve government performance. It is time to move to an information age government. The Commission is considering several options for how best to achieve this. Our view is that this new model of governance must be based in the Executive Office of the President and make collaboration among agencies one of its missions.

### **Public-Private Partnerships**

The Committee knows that the U.S. works with a variety of groups created to improve information sharing or build public private partnerships. Based on a series of interviews, we found almost universal recognition that the status quo is not meeting the needs of government or the private sector with respect to collaboration.

Our work concentrated on two problems that must be addressed if there is to be improvement. The first is to rebuild trust between the government and the private sector. The second is to focus on infrastructures that are truly critical for cyber security - the sectors that provide the large national networks that create cyberspace – telecommunications, electricity, and finance.

We heard in numerous interviews that trust is the foundation of a successful government/private sector relationship. We also heard that in the last few years, despite the profusion of advisory bodies and despite good intentions on all sides, trust between government and the private sector has declined. Our recommendations will call for simplifying structure and building trust relationships. Information sharing, which drove much of the original thinking about how to work with the private sector, should become a secondary goal in our view.

### **Regulation**

Our group had a long debate over the role of regulation and whether there has been market failure in cyber security. Our conclusion is that greater regulation is necessary, but that prescriptive, command-and-control regulation will not produce a higher standard for security in critical cyber infrastructure. We are exploring a new approach to regulation that builds on and blends the strengths of the public and private sectors.

Based on this Committee's hearings on NERC and FERC, we are exploring approaches that build on your vision of how NERC/FERC should work. This approach would task existing regulatory agencies for telecommunications, finance, and electrical power to devise regulations

that embed cyber security requirements in a regulatory and compliance framework. To achieve this while avoiding the drawbacks of regulation, the Federal government must find new ways to coordinate among agencies. We plan to recommend a “federated” approach to regulation that reduces the fragmentation and inconsistency found in cyber security regulation.

### **Identity and attribution**

One of the new regulations we think are necessary for cyber security involve authentication of identity for critical infrastructures in cyberspace. The current internet is anonymous. Anonymity can preserve privacy and civil liberties, but it can also enable malicious behavior. We have concluded that the government must require better authentication for critical infrastructure, and that this can be done in a way that protects privacy and confidentiality.

We started with the principle that unknown individuals or individuals using fraudulent identities should not be able to easily access critical infrastructure. We are developing a technology-neutral, “opt-in” approach to digital credentials for critical infrastructure, based on precedents from the work of the FDIC and the experience of the Department of Defense.

Our view is that it will be feasible to create a system where those who did not want to be authenticated could choose not to participate without penalty, but those who offer online services and wished to restrict them to authenticated individuals would not have that right denied to them. We recognize the sensitivity of any recommendation to require authentication and believe that no measure that does not adequately protect civil liberties will succeed, but we have concluded that security cannot be improved without better authentication of identity.

### **Modernize authorities for cyberspace**

We heard many times in our interviews that a legal structure that is a decade or two old ill-serves the nation when it comes to cyber security. Some of this is due to transaction speed – an event in cyberspace may happen in seconds, but determining which authority to use in response can take hours or days (and we heard that the “default” authority is Title 3 – law enforcement – as this is the set of authorities that is least likely to pose risks for civil liberties).

We believe that the next administration should work with Congress to revise three authorities: Title 3 investigative authorities related to cyber space; the Clinger-Cohen Act and the Federal Information Security Management Act; and the distinction in law between national security and civilian agency systems currently embedded in many authorities. Revising existing authorities to serve the nation effectively in cyber space will be a complex legal operation that will require Congress and the new administration to work closely together, but it is an unavoidable challenge.

### **Resources and Incentives**

Our discussions and interviews suggest that the Federal government has not made full use of its powers to change market conditions in ways that will improve cyber security. It can increase the inputs and resources available for cyber security by supporting training and education. It can expand and focus its investment in research. It can encourage the deployment of more secure products and protocols by using its purchasing power – the federal government does not have a

dominant market share in IT, but it is the largest single customer for most IT products and it can use this to move the market in positive directions.

Our recommendations will call for changes in acquisitions requirements, collaborative work with companies on standards and best practices, and investment in human capital and in research to accelerate the rate at which we secure cyberspace. In this, we will recommend that a new administration build off OMB's Federal Desktop Core Configuration initiative.

Cooperation with private sector will be essential for success. Leveraging government and industry partnerships can produce major improvements in security. Moreover, the development of more secure configurations must involve those international standards bodies who have been working in this area.

Our review suggests that the U.S. would benefit if it developed a national cyber education and training program. Our recommendation is that the U.S. develop an institutionalized program that establishes minimal standards for skills and knowledge sufficient to meet the cyber mission and enable attractive career paths.

The Federal government is one of the largest purchasers of telecommunications services in the world – perhaps the largest. A presidential mandate that the U.S. would only contract with telecommunications carriers that use DNS SEC would rapidly drive the market and provide benefits beyond the Federal government. This recommendation is attractive because it could also be adopted by state and local governments.

### **Information Assurance Metrics**

A central part of any effort to judge whether a product or initiative has improved security is to identify or develop the metrics that can measure progress. There is no doubt that achieving compliance with best security practice is a basic foundation that is valuable and should be measured - what we lack is the ability to go beyond that with meaningful measures of security that inform the system owner on their actual risk profile, and how best to make intelligent investments in making the IT system more secure and reducing the overall risk.

### **Assuring Industrial Control System Cyber Security**

Industrial Control Systems (also known as SCADA) are an integral part of electric power, oil, water, gasoline, chemicals, manufacturing, mining, transportation, food processing, etc. by providing control and safe shutdown of the processes for these facilities. Computer cyber vulnerabilities can affect the safe, functional performance of these systems and processes. We are working with experts in this field to develop recommendation on how to improve the security of ICS. These recommendations will probably be linked to our recommendation to develop a new regulatory approach for cyber security.

### **Research and Development for Cyber Security**

Although technology is only a part of the cybersecurity challenge, the next administration has an opportunity to use research and development to improve the security of computer and communications systems and the information created and stored within them.

Our initial work suggests that the U.S. needs a coordinated and strategic focus for Federal investments in cyber security R&D. Both basic research—often performed at universities and with benefits realized over the long term—and applied research— which uses existing technology to address near-term problems—must be part of this strategy. Just as the Department of Defense has successfully marshaled R&D to provide military advantage to the U.S. since the 1940s, the U.S. must harness R&D to America’s cybersecurity needs

One area we are considering for R&D involves re-engineering the Internet, which operates with protocols written in the 1970s and 1980s. A simple analogy would be to ask if it is safe to drive a thirty year old car that still uses its original equipment. WE believe it is time to upgrade. Many of outside experts suggested that we remember that cyberspace is a human construct and that the Internet’s architecture, with research and international cooperation, can be significantly improved. This is a bold and complex recommendation that will require a coordinated effort managed by the White House as part of a larger strategy, but it is not out of reach.

### **Next Steps**

The Commission’s goal is a package of implementable recommendations that could help to guide both a legislative agenda and Presidential policy documents. We are on track to have this done within the next two months. Several difficult issues remain, including how to move from an industrial age model of governance to one better suited for the information age, how to scope and design a new approach to regulation, where to locate the authorities for cyberspace within the Federal government, and how to make public-private partnership more efficient. I am confident that with your help and guidance we can resolve these issues and offer our recommendation to the next administration, the Congress and the American public. Thank you again for this opportunity and I would be happy to take any questions you may have.